

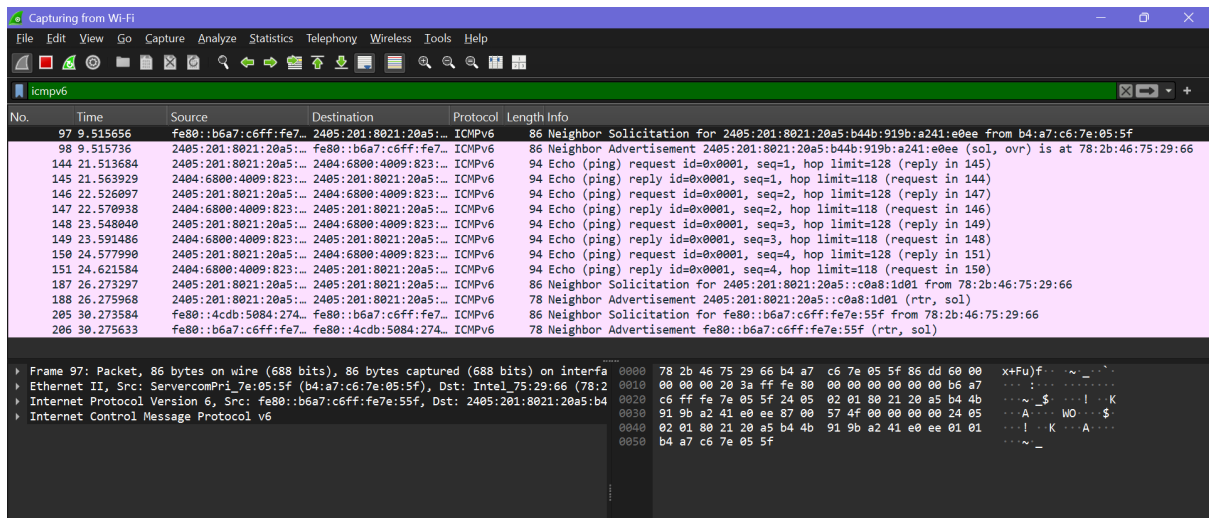
Jadavpur University
Department of Computer Science
and Engineering



NETWORKS LAB
ASSIGNMENT 5

BCSE UG-III

Student : Arjeesh Palai
Roll No. : 002310501086
Group : A3
Date : 10 / 11 / 2025



Answer: Started a fresh capture and ran ping. L2 resolution precedes ICMP: ARP (IPv4) or ICMPv6 ND (IPv6). After resolution, Echo Request/Reply pairs appear for the ping exchange.

Q2. Web traffic inspection (protocols, RTT, addresses, Host)

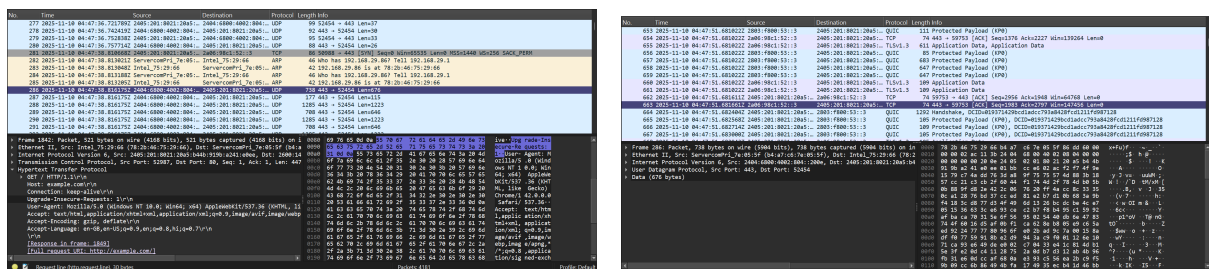
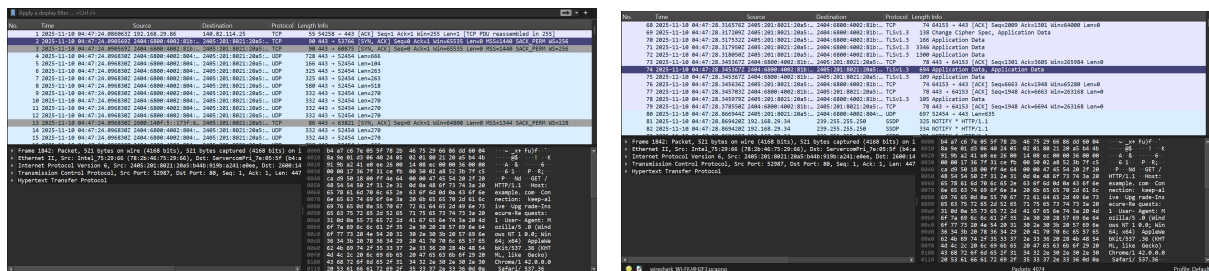


Figure 4: Unfiltered protocol glimpses (2/3).

No.	Time	Source	Destination	Protocol	Length	Info
4576	2025-11-10 04:55:44.1732332	192.168.29.86	35.186.199.248	TCP	54	60970 → 443 [ACK] Seq=2119 Ack=831 Win=64512 Len=0
4577	2025-11-10 04:55:44.2520722	2405:201:8021:20a5::...	2a06:98c1:52::3	QUIC	1292	Initial, DCID=1621543b50b70f13, PKN: 38, PING, PING, PADDING, PING, CRYPTO, CRYPT...
4578	2025-11-10 04:55:44.2839332	2405:201:8021:20a5::...	2405:201:8021:20a5::...	DNS	187	Standard query 0x5e4a HTTPS safebrowsing.googleapis.com
4579	2025-11-10 04:55:44.2843182	2405:201:8021:20a5::...	2405:201:8021:20a5::...	DNS	187	Standard query 0xf5c2 AAAA safebrowsing.googleapis.com
4580	2025-11-10 04:55:44.2846272	2405:201:8021:20a5::...	2405:201:8021:20a5::...	DNS	187	Standard query 0xfdb1 A safebrowsing.googleapis.com
4581	2025-11-10 04:55:44.2850242	192.168.29.86	1.1.1.1	DNS	85	Standard query 0x9178 HTTPS chrome.cloudflare-dns.com
4582	2025-11-10 04:55:44.2853892	192.168.29.86	1.1.1.1	DNS	85	Standard query 0x7441 AAAA chrome.cloudflare-dns.com
4583	2025-11-10 04:55:44.2855612	192.168.29.86	1.1.1.1	DNS	85	Standard query 0xe67f A chrome.cloudflare-dns.com
4584	2025-11-10 04:55:44.2910562	1.1.1.1	192.168.29.86	DNS	117	Standard query response 0xe67f A chrome.cloudflare-dns.com A 172.64.41.3 A 162.15...
4585	2025-11-10 04:55:44.2920862	1.1.1.1	192.168.29.86	DNS	141	Standard query response 0x7441 AAAA chrome.cloudflare-dns.com AAAA 2803:f800:53::...
4586	2025-11-10 04:55:44.2920862	1.1.1.1	192.168.29.86	DNS	158	Standard query response 0x9178 HTTPS chrome.cloudflare-dns.com HTTPS
4587	2025-11-10 04:55:44.2941462	2405:201:8021:20a5::...	2803:f800:53::3	QUIC	1292	Initial, DCID=f2b56bd39d49842f, PKN: 1, PADDING, CRYPTO, CRYPTO, PADDING, PING, C...
4588	2025-11-10 04:55:44.2942792	2405:201:8021:20a5::...	2803:f800:53::3	QUIC	1292	Initial, DCID=f2b56bd39d49842f, PKN: 2, PING, CRYPTO, CRYPTO, PADDING, CRYPTO, CR...
4589	2025-11-10 04:55:44.2945042	2405:201:8021:20a5::...	2803:f800:53::3	QUIC	139	0-RTT, DCID=f2b56bd39d49842f
4590	2025-11-10 04:55:44.3304732	2405:201:8021:20a5::...	2803:f800:53::3	QUIC	1292	Initial, DCID=f2b56bd39d49842f, PKN: 5, PADDING, CRYPTO, PADDING, PING, PING, CRY...

Frame 668: Packet, 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface
Ethernet II, Src: Intel_75:29:66 (78:2b:46:75:29:66), Dst: ServercomPri_7e:05:5f (b4:a
Internet Protocol Version 6, Src: 2405:201:8021:20a5:b44b:919b:a241:e0ee, Dst: 2803:f8
User Datagram Protocol, Src Port: 55735, Dst Port: 443
QUIC IETF

0000 b4 a7 c6 7e 05 5f 78 2b 46 75 29 66 86 dd 60 05 ... x Fu f
0010 fd 20 00 37 11 40 24 05 02 01 80 21 20 a5 b4 4b ... 7 05 ... K
0020 91 9b a2 41 e0 ee 26 00 14 08 ec 00 00 36 00 00 ... A & ... 6
0030 00 00 17 36 7f 31 ce fb 00 50 02 a8 52 3b 7f c5 ... 6 1 ... P R
0040 48 54 54 58 2f 31 2e 81 00 00 48 6f 73 74 3a 20 ... P Nd GET /
0050 65 78 61 6d 70 6c 65 2e 63 6f 6d 0a 43 6f 6e ... HTTP/1.1 Host:
0060 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c ... example.com Con
0070 69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 ... nection: keep-al
0080 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 ... ive Upg rade-Ins
0090 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d ... equire-Re quests:
00a0 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 ... 1 User- Agent: M
00b0 6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e ... ozilla/5.0 (Wind
00c0 36 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57 65 ... ows NT 1.0.0; Win
00d0 62 4b 69 74 2f 35 33 37 2e 33 36 20 20 4b 48 54 ... 64; x64) AppleWe
00e0 4d 4c 2c 20 6c 69 0b 65 20 47 65 63 6b 6f 29 20 ... bkit/537.36 (KHT
00f0 43 68 72 6f 6d 65 2f 31 34 32 2e 30 2e 30 2e 30 ... ML, like Gecko)
0100 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f ... Chrome/142.0.0.0

Figure 5: Unfiltered protocol glimpses (3/3).

No.	Time	Source	Destination	Protocol	Length	Info
1842	2025-11-10 04:48:38.1173022	2405:201:8021:20a5::...	2600:1408:ec00:36::...	HTTP	521	GET / HTTP/1.1
1849	2025-11-10 04:48:38.1733279	2600:1408:ec00:36::...	2405:201:8021:20a5::...	HTTP	768	HTTP/1.1 200 OK (text/html)
1879	2025-11-10 04:48:38.5247652	2405:201:8021:20a5::...	2600:1408:ec00:36::...	HTTP	461	GET /favicon.ico HTTP/1.1
1895	2025-11-10 04:48:39.1342182	2600:1408:ec00:36::...	2405:201:8021:20a5::...	HTTP	978	HTTP/1.1 404 Not Found (text/html)

Figure 6: HTTP GET packet used for latency measurement.

No.	Time	Source	Destination	Protocol	Length	Info
1842	2025-11-10 04:48:38.1173022	2405:201:8021:20a5::...	2600:1408:ec00:36::...	HTTP	521	GET / HTTP/1.1
1849	2025-11-10 04:48:38.1733279	2600:1408:ec00:36::...	2405:201:8021:20a5::...	HTTP	768	HTTP/1.1 200 OK (text/html)
1879	2025-11-10 04:48:38.5247652	2405:201:8021:20a5::...	2600:1408:ec00:36::...	HTTP	461	GET /favicon.ico HTTP/1.1
1895	2025-11-10 04:48:39.1342182	2600:1408:ec00:36::...	2405:201:8021:20a5::...	HTTP	978	HTTP/1.1 404 Not Found (text/html)

Frame 1842: Packet, 521 bytes on wire (4168 bits), 521 bytes captured (4168 bits) on interface
Ethernet II, Src: Intel_75:29:66 (78:2b:46:75:29:66), Dst: ServercomPri_7e:05:5f (b4:a
Internet Protocol Version 6, Src: 2405:201:8021:20a5:b44b:919b:a241:e0ee, Dst: 2600:14
Transmission Control Protocol, Src Port: 52987, Dst Port: 80, Seq: 1, Ack: 1, Len: 447
Hypertext Transfer Protocol

0000 b4 a7 c6 7e 05 5f 78 2b 46 75 29 66 86 dd 60 04 ... x Fu f
0010 8a 9e 01 d3 06 40 24 05 02 01 80 21 20 a5 b4 4b ... 05 ... K
0020 91 9b a2 41 e0 ee 26 00 14 08 ec 00 00 36 00 00 ... A & ... 6
0030 00 00 17 36 7f 31 ce fb 00 50 02 a8 52 3b 7f c5 ... 6 1 ... P R
0040 ca d9 50 18 00 ff 4e 64 00 00 47 45 54 20 2f 20 ... P Nd GET /
0050 48 54 54 58 2f 31 2e 81 00 00 48 6f 73 74 3a 20 ... HTTP/1.1 Host:
0060 65 78 61 6d 70 6c 65 2e 63 6f 6d 0a 43 6f 6e ... example.com Con
0070 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c ... nection: keep-al
0080 69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 ... ive Upg rade-Ins
0090 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 ... equire-Re quests:
00a0 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d ... 1 User- Agent: M
00b0 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 ... ozilla/5.0 (Wind
00c0 6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e ... ows NT 1.0.0; Win
00d0 36 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57 65 ... 64; x64) AppleWe
00e0 62 4b 69 74 2f 35 33 37 2e 33 36 20 20 4b 48 54 ... bkit/537.36 (KHT
00f0 4d 4c 2c 20 6c 69 0b 65 20 47 65 63 6b 6f 29 20 ... ML, like Gecko)
0100 43 68 72 6f 6d 65 2f 31 34 32 2e 30 2e 30 2e 30 ... Chrome/142.0.0.0

Figure 7: Matching HTTP 200 OK reply with timestamp.

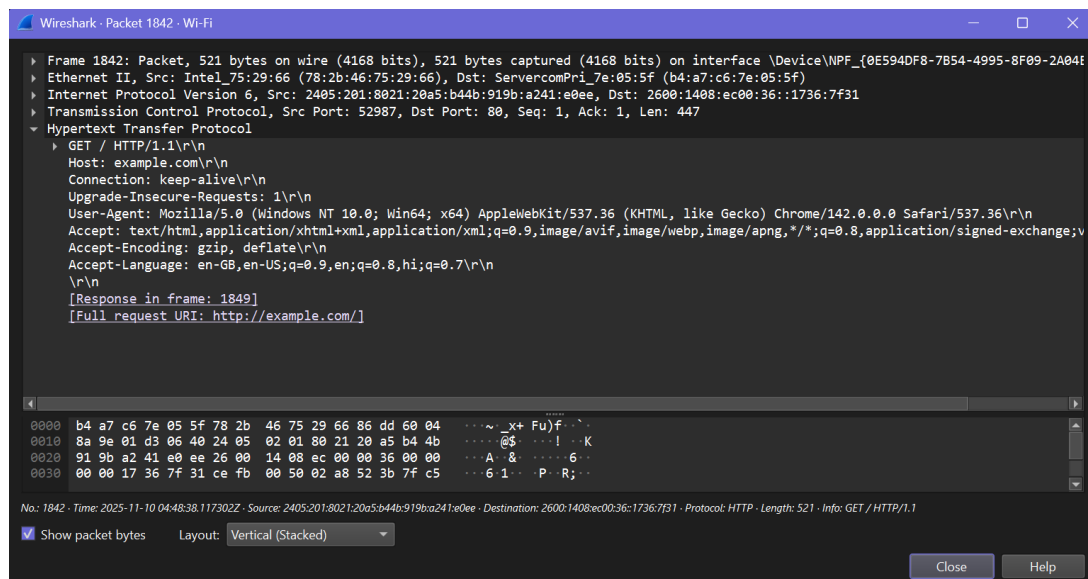


Figure 8: Source/Destination IPs from the GET packet.

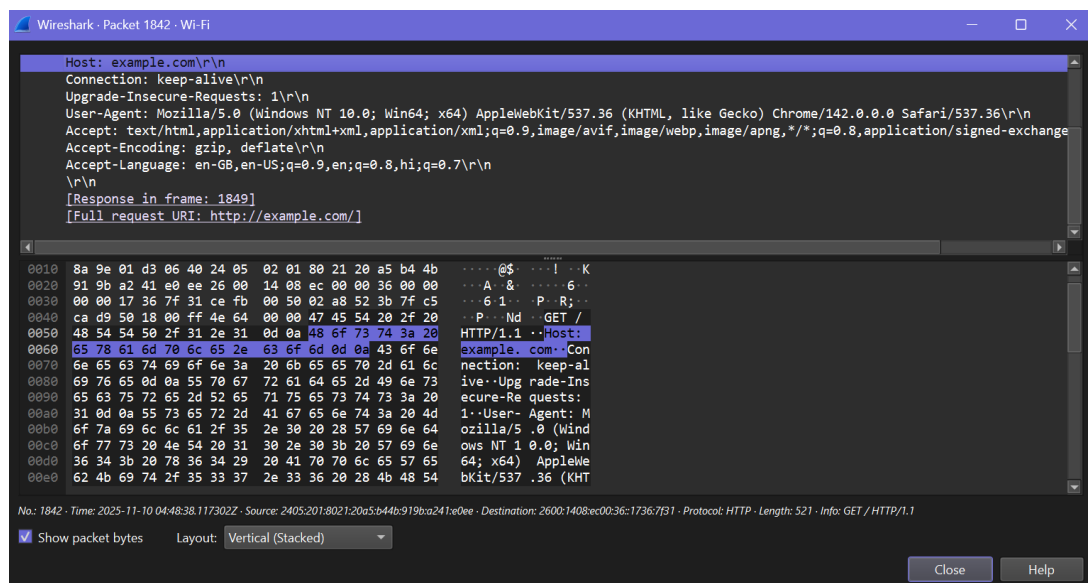


Figure 9: Packet Bytes and HTTP header showing Host :.

- (a) **Protocols:** TCP, UDP, HTTP, ARP, DNS, TLS 1.2/1.3, QUIC, SSDP, ICMPv6.
- (b) **HTTP latency:** GET at $t = 74.031239$ s; 200 OK at $t = 74.331279$ s $\Rightarrow \Delta t = 0.30004$ s.
- (c) **IPs:** Source (host) 2405:201:8021:20a5:b44b:919b:a241:e0ee; Destination (site) 2600:1408:ec00:36::1736:7f31.
- (d/e) **Host:** Host: example.com in the HTTP layer.

Q3. Hex and ASCII in Packet Bytes

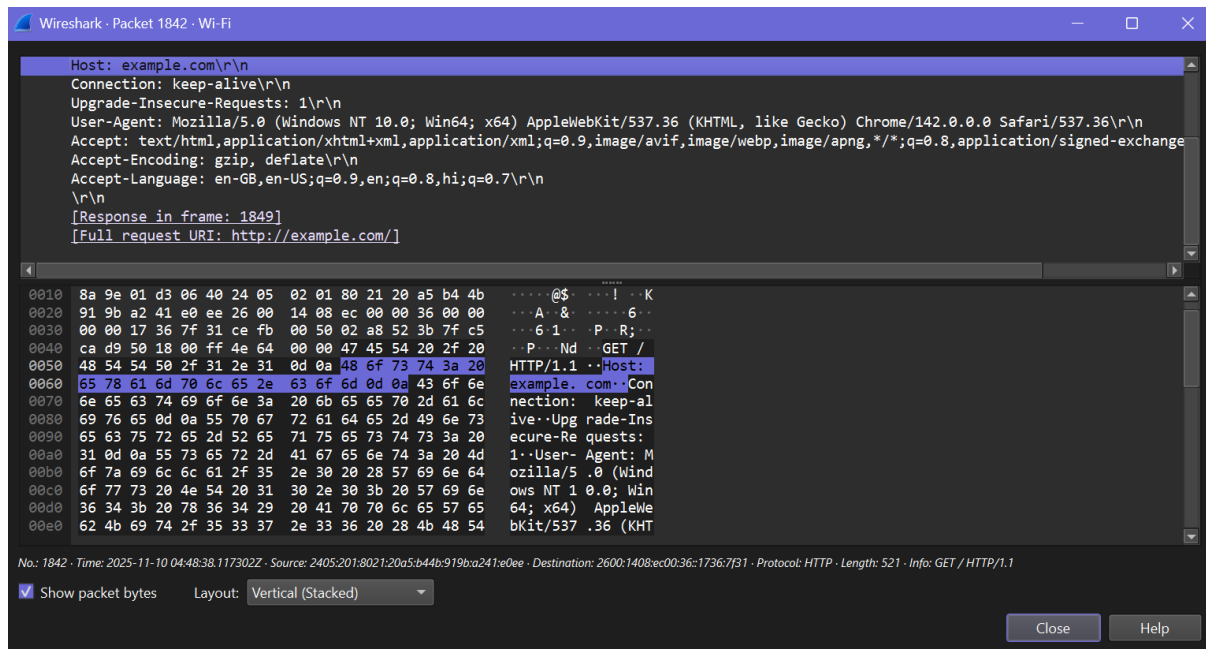


Figure 10: Packet Bytes pane showing aligned Hex and ASCII.

Answer: The lower pane displays offset, hex bytes, and ASCII; the Host: example.com substring is visible with matching hex.

Q4. First 4 bytes of Hex for the Host value

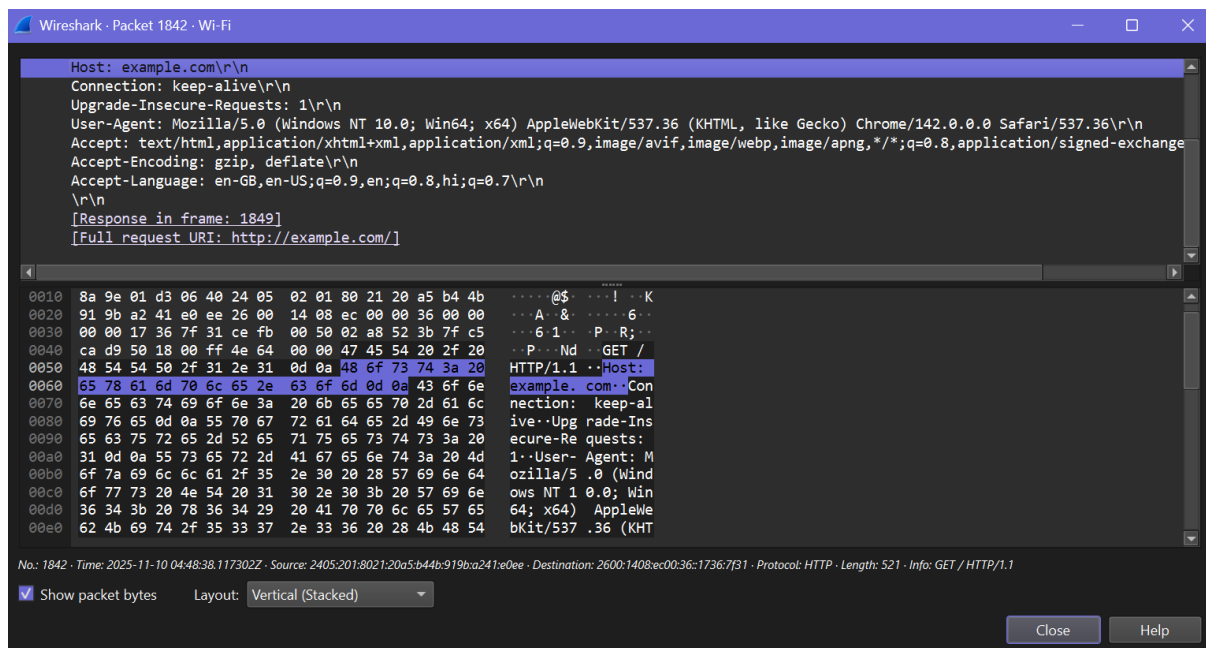


Figure 11: Locating the start of example.com for hex extraction.

Answer: The first four bytes of the value (*exam*) are **65 78 61 6d**.

Q5. Follow a conversation (flow)

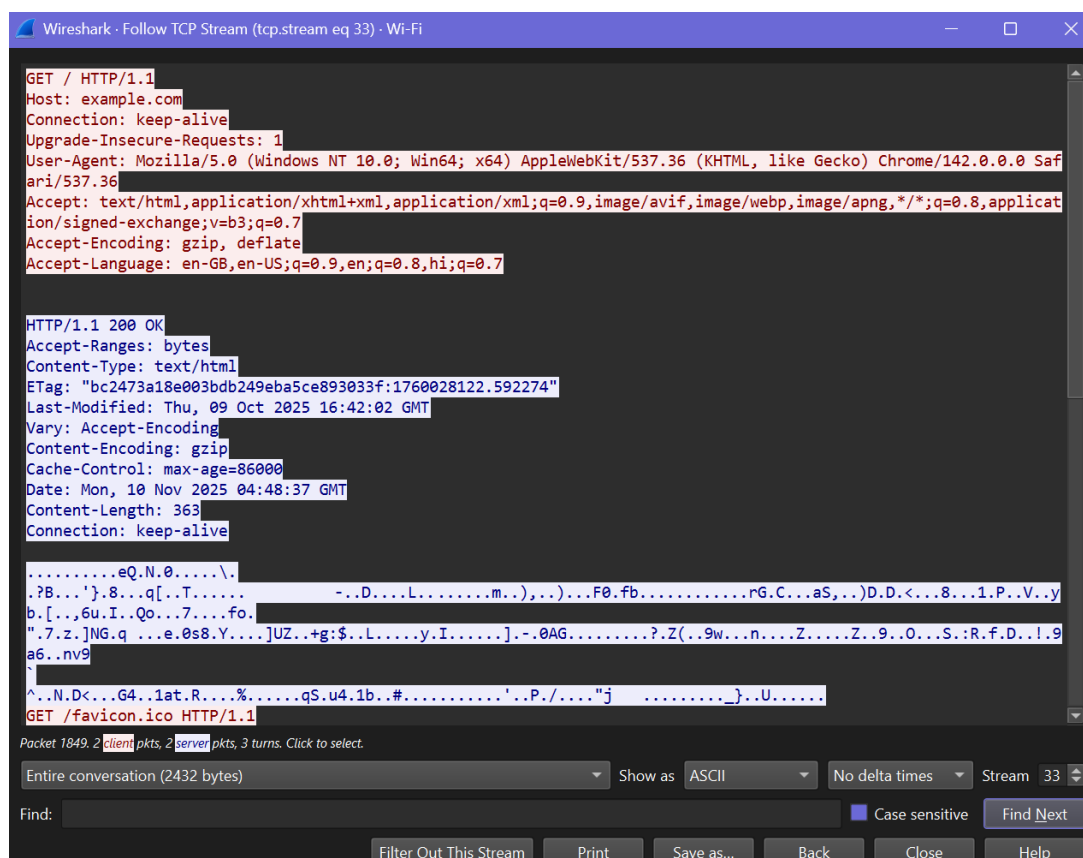


Figure 12: Follow → TCP Stream: reassembled request.

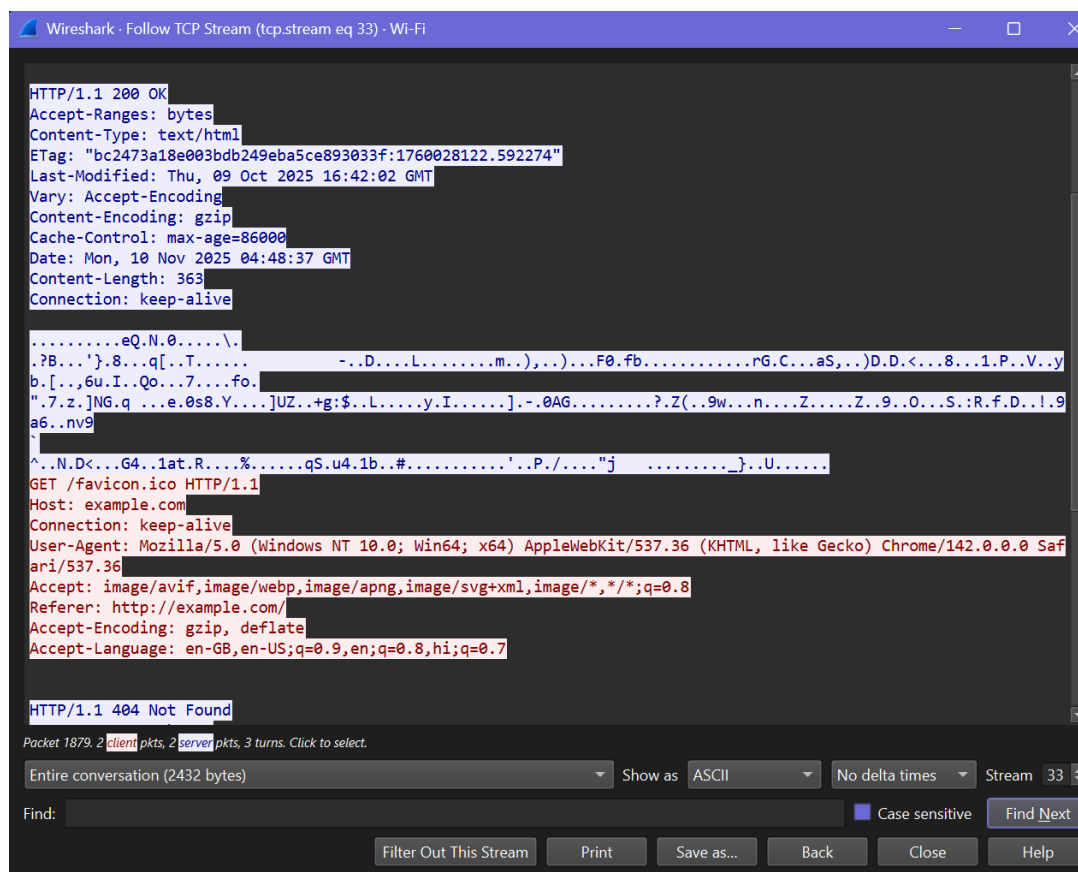


Figure 13: Follow → TCP Stream: reassembled response.

Answer: Using Follow TCP Stream reconstructs the HTTP GET and the subsequent 200 OK with payload.

Q6. HTTP packet from server (TCP Source Port = 80)

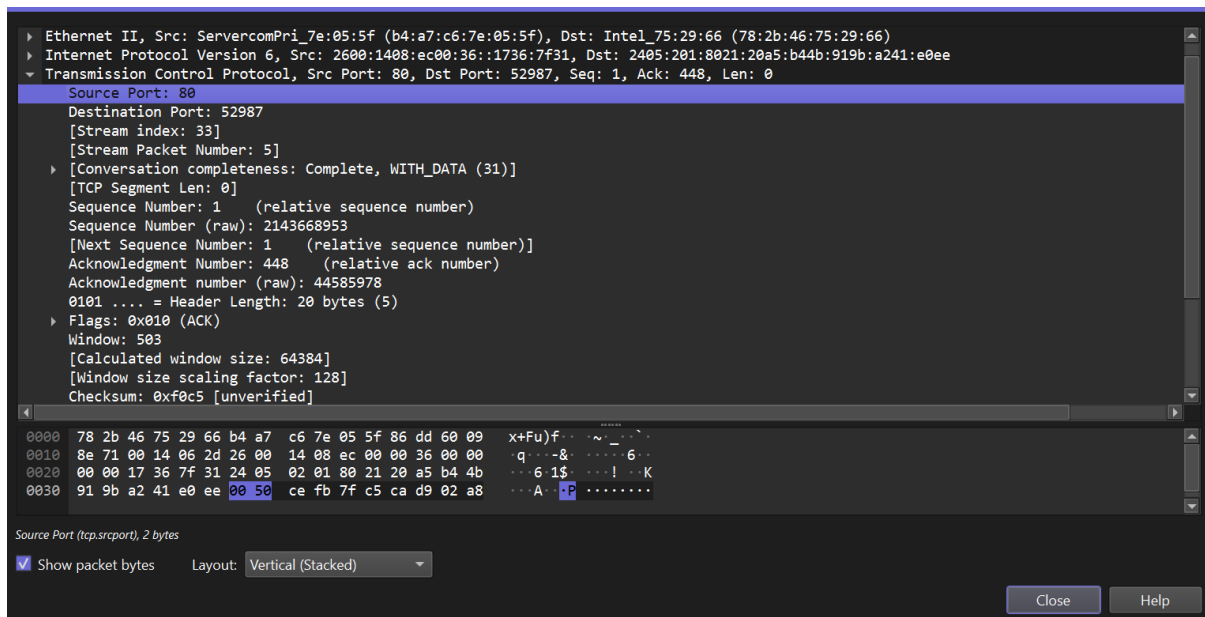


Figure 14: Server → client segment with TCP Src=80 and Ethernet expanded.

Answer: A server-to-client HTTP packet shows TCP Source Port = 80; expanding Ethernet reveals MAC addressing.

Q7. NIC manufacturers (vendor resolution)

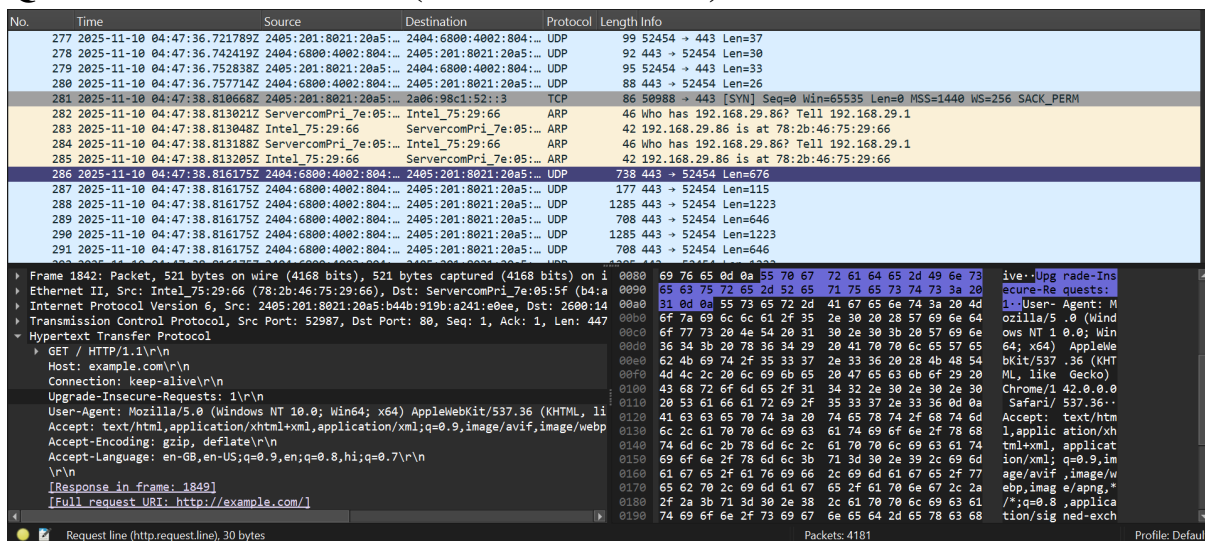


Figure 15: Ethernet II details with vendor names (name resolution enabled).

Answer: Vendor mapping indicates the host NIC as **Intel** and the server NIC as **ServercomPri** (example frames shown).

Q8. Hex OUIs (first three bytes of each MAC)

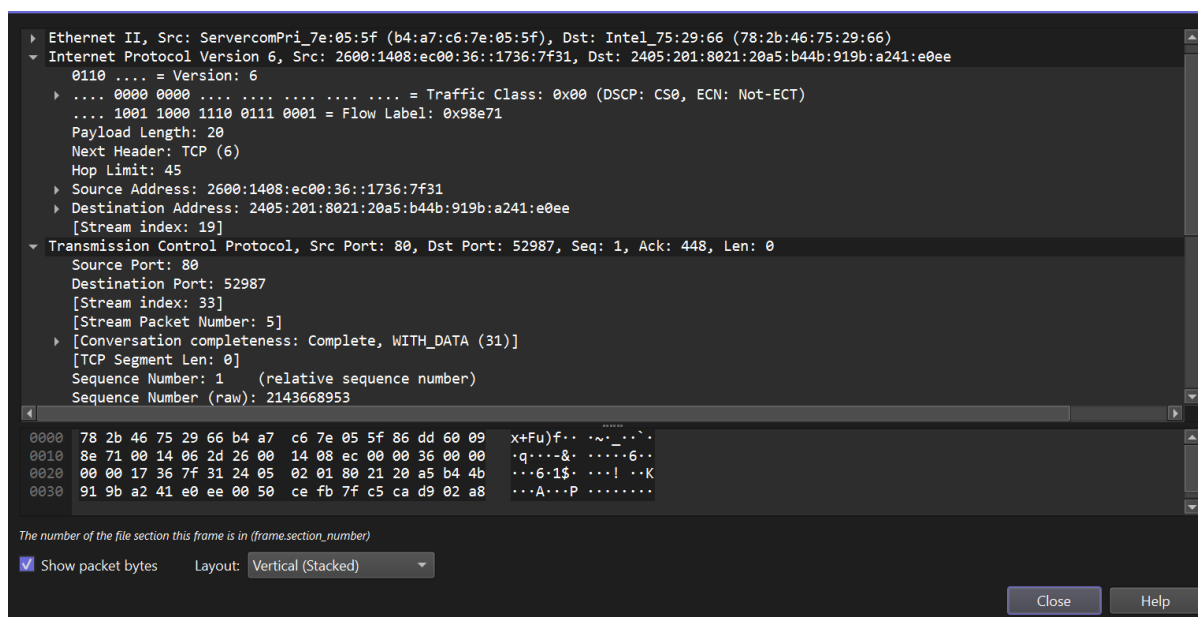


Figure 16: Reading OUIs (first 3 bytes) from MAC addresses.

Answer: OUIs observed: Intel **78 : 2b : 46**; ServercomPri **b4 : a7 : c6**.

Q9. Protocol percentages (TCP vs UDP)

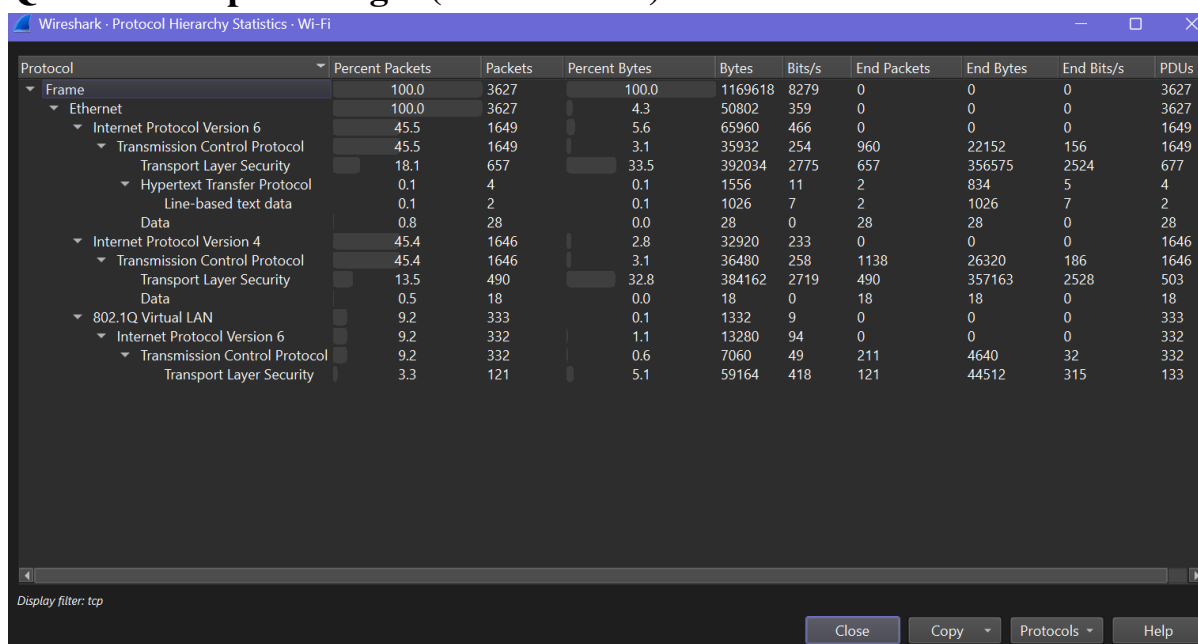


Figure 17: Protocol Hierarchy (capture must be unfiltered).

Answer: Clear display filters → **Statistics** → **Protocol Hierarchy** to obtain accurate TCP/UDP percentages for the entire capture.

Q10. Flow Graph

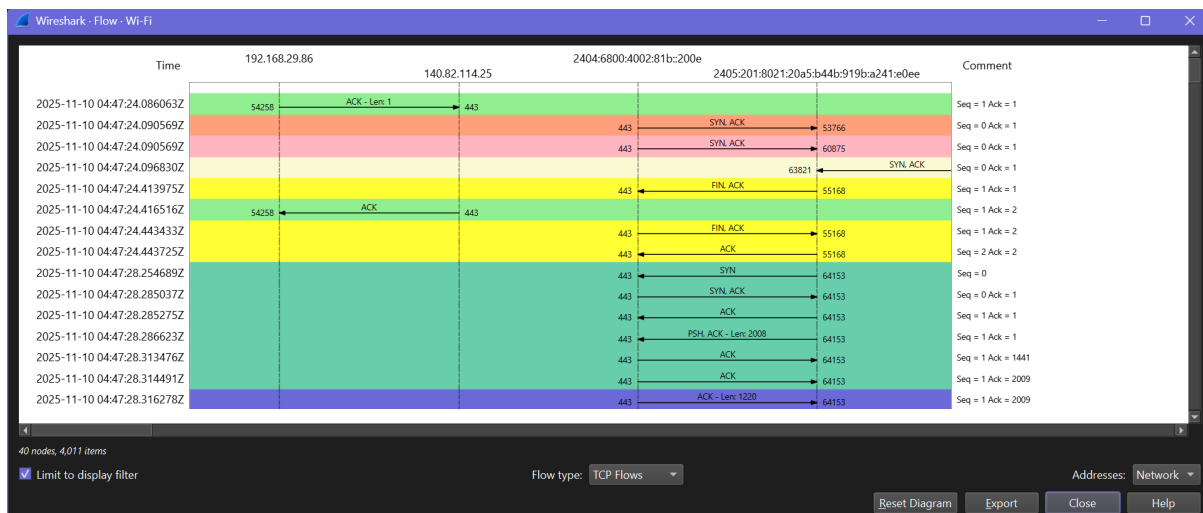


Figure 18: Statistics → Flow Graph summarizing per-flow timelines.

Answer: The graph shows SYN/SYN-ACK/ACK transitions and request/response ordering across concurrent connections.

Appendix: Capture Steps

- Selected the correct NIC and started capture.
- Enabled MAC name resolution for vendor IDs.
- Generated traffic: ping, web browsing (HTTP/HTTPS), DNS lookups.
- Used filters (http, tcp, dns), Follow Streams, Protocol Hierarchy, and Flow Graph.